## REMARKS

Examiner has rejected Claims 5-6 as being indefinite under 35 U.S.C. 112. In response, Applicant has canceled Claims 5-6.

Examiner has rejected Claims 1-6 as being unpatentable under 35 U.S.C. 103 over U.S. Publication No. 2002/0099944 ("Bawlin") in view of U.S. Publication No. 2003/0153070 ("Mayer") . Applicant respectfully disagrees with the Examiner. Applicant has canceled Claims 2 and 4-6, combined the canceled claim 2 to base claim 1.

Bawlin discloses methods and an apparatus which enable a computer user to prevent unauthorized access to the files stored on a computer. The apparatus comprises a computer for storing and managing security-sensitive files, a first database for identifying files stored on the computer which are to be included in a safe zone, a second database for defining authorized access to the files within the safe zone, and a filter for determining whether the file to be accessed is within the safe zone. The methods and apparatus are a technology for, when access to a file is attempted, determining whether to allow the access by determining whether the access is authorized.

Mayer discloses a system and method for protecting information and performing a security function by preventing access by malicious programs, and provides a technology for, in order to enable a certain function invoked for specific signal or data processing to be executed only when specific conditions are met, hooking that certain function and then enabling execution of the specific function to be resumed if it is determined that the specific conditions are met.

Whereas, the instant application discloses an access control system, comprising a Virtual Secure Disk (VSD) image file module occupying a certain space of a hard disk in a file form; a VSD drive for processing security-sensitive files within the VSD image file module; an encryption and decryption module for encrypting and decrypting data input, output, or input and output between the VSD image file module and the VSD drive; a VSD file system module for allowing an operating system to recognize the VSD drive as a separate disk volume at a

time of access to the security-sensitive files within the VSD image file module; and an access control module for determining access by determining whether an access location is a disk drive or the VSD drive and an application module has been authorized to access a file, which is stored on the hard disk, to perform tasks in the application module, wherein an authorized application module is configured to access the disk drive for write and read operations, wherein the authorized application module is configured to access the disk drive for a read operation only, wherein an unauthorized application module is configured to access the disk drive for write and read operations, and wherein the unauthorized application module is not allowed to access the VSD drive;

wherein the access control module comprises an extended system service table for allowing the operation of a corresponding function to be performed when it is pointed at by a descriptor, and an extended system table for changing a function, which is requested of the service system table by the application module, to prevent operation of the function, determining whether a space in which a corresponding task is performed is the disk drive or the VSD drive, determining whether access to the corresponding file by the application module has been authorized, and providing an unchanged function to the extended system service table or stopping the operation of the function according to results of the determination.

Reasons Why the Instant Application has Non-Obviousness over Bawlin and Mayer

<1>

- The instant application enables authorized and unauthorized applications to normally run on the same system. In particular, an authorized application is enabled to run both on the VSD drive, which is a secure area, and on the disk drive, which is an insecure area.

- Meanwhile, if an authorized application were able to run on both the VSD drive and on the disk drive and, particularly, were able to perform a write operation on the disk drive, the content of the security-sensitive files stored on the VSD drive could be copied to the disk drive by a malicious user.

- Accordingly, the instant application is technically configured such that an authorized application can perform only a read operation on the disk drive but cannot perform a write operation thereon.

- As a result, an authorized application according to the instant application can execute a security-sensitive file of the VSD drive and a general file of the disk drive at the same time in a single execution, so that the convenience and efficiency of applying the content of the general file to the security-sensitive file and the security of preventing the content of the security-sensitive file from being applied to the content of the general file can be anticipated.

- This technical construction is clearly different from the technology of Bawlin which is configured to determine whether an application accessing the safe zone has been authorized, and also the construction for achieving the effects of the instant application cannot be found anywhere in the specification of Bawlin.

<2>

- The extended system service table of the instant application replaces the conventional system service table which a descriptor approaches such that an application points at a function. When an authorized or unauthorized application requests a function from the OS, the OS provides the corresponding function to the extended system service table, and the extended system service table changes the function and checks (1) to (5) of the access control module, thereby determining whether to restore the function to its original form.

- The non-obviousness of the instant application was denied based on the "first and second databases" disclosed in Bawlin and the "hooking" disclosed in Mayer.

- However, the extended system service table of the instant application presents constituent elements for actually processing functions, other than functional elements such as the "first and second databases" described in Bawlin and the "hooking" described in Mayer. In particular, the present invention presents a technical example in which the constituent elements presented as described above enable an authorized application to run both on the VSD drive and the disk drive, and limit the function of performing a write operation on the disk drive. The person skilled in the art could not easily invent the substantially associated operation between the extended system service table and descriptor of the instant application based on Bawlin and Mayer in which only functional expressions such as "the functions of the first and second databases" and "hooking function" have been described.

- In greater detail, the extended system service table of the instant application replaces the conventional system service table, so that the OS provides a function to the extended system

service table, rather than the conventional system service table, and only an authorized application includes functions of changing and restoring a function so that the authorized application can point at the corresponding function in the extended system service table.

- In contrast, the 'hooking function' is a function of intercepting corresponding data or a corresponding signal on a path for the data or signal, thereby preventing an object (application or the like) from receiving the data or signal, and is a technology for controlling the processing of data or a signal while maintaining the predetermined path for the data or signal.

- As a result, the extended system service table of the instant application does not require the task of intercepting a corresponding function midway by changing the function provision path of the OS, unlike the 'hooking function', and the changing and restoring of a function is indispensably performed before a corresponding application points at the OS using a descriptor. The construction of the extended system service table has little relation with the 'hooking function'.

<3>

- Therefore, Applicant submits that the amended claims 1 and 3 are not obvious over the cited references. Applicant respectfully requests withdrawal of the rejections.

Conclusion

In view of the amendments and remarks made above, it is respectfully submitted that claims 1 and 3 are in condition for allowance, and such action is respectfully solicited, if required, under *Examiner's Amendment*.

Respectfully submitted,

Date: October 2, 2009

/James E. Bame/

James E. Bame
Regis. No. 44521
Tel: 213-384-7200
IPLA P.A.
3580 Wilshire Blvd 17th Fl.
Los Angeles, CA 90010